RSA PAM Module Installation on RHEL OS Platform

Preparation

Copy the tar file, `AuthenticationAgent_60_PAM_95_060308.tar`, to an installation directory and untar it.

```
# tar xvf ./AuthenticationAgent_60_PAM_95_060308.tar
aix/
aix/sd_pam_agent.tar
hp11/
hp11/sd_pam_agent.tar
hpitan/
hpitan/sd_pam_agent.tar
install_pam.sh
license.txt
license2.txt
lnx32/
lnx32/sd_pam_agent.tar
lnx64/
lnx64/sd_pam_agent.tar
PAMAgent.pdf
PAMreadme.pdf
solsparc/
solsparc/sd_pam_agent.tar
solx86/
solx86/sd_pam_agent.tar
uninstall_pam.sh
```

Prepare PAM Module Run Time Environment

Download `sdconf.rec` file.

On the RedHat Linux Authentication Agent:

```
# mkdir /var/ace
# cp ./sdconf.rec /var/ace/
# VAR_ACE="/var/ace/"
# echo $VAR_ACE
/var/ace/
# vi /var/ace/sdopts.rec

CLIENT_IP=<host_IP_address>
```

(Save and exit.)

Installation

```
# ./install_pam.sh

ARE YOU A CUSTOMER ORDERING THIS RSA PRODUCT FROM RSA SECURITY INC., FROM
EITHER NORTH AMERICA, SOUTH AMERICA OR THE PEOPLE'S REPUBLIC OF CHINA
(EXCLUDING HONG KONG): (y/n) [y] <Return>

LICENSE AGREEMENT

***   IMPORTANT   ***
PLEASE READ CAREFULLY BEFORE CONTINUING WITH THIS INSTALLATION.  AT THE END
OF THE LICENSE TERMS AND CONDITIONS STATED BELOW, CUSTOMER WILL BE ASKED TO
ACCEPT OR REJECT SUCH TERMS.  BY INDICATING ITS ACCEPTANCE, CUSTOMER AGREES
TO BE BOU
ND BY THE TERMS OF THIS LICENSE AGREEMENT.

<skipped>

**************************************************

Do you accept the License Terms and Conditions stated above? (Accept/Decline)
[D]Accept


Enter Directory where sdconf.rec is located [/var/ace] <Return>


Please enter the root path for the RSA Authentication Agent for PAM directory
[/opt] <Return>

The RSA Authentication Agent for PAM will be installed in the /opt directory.
pam/
pam/doc/
pam/lib/
pam/lib/pam_securid.so
pam/bin/
pam/bin/acestatus
pam/bin/acetest

Checking /etc/sd_pam.conf:

VAR_ACE does not exist - entry will be appended
ENABLE_GROUP_SUPPORT does not exist - entry will be appended
INCL_EXCL_GROUPS does not exist - entry will be appended
LIST_OF_GROUPS does not exist - entry will be appended
PAM_IGNORE_SUPPORT does not exist - entry will be appended
AUTH_CHALLENGE_USERNAME_STR does not exist - entry will be appended
AUTH_CHALLENGE_RESERVE_REQUEST_STR does not exist - entry will be appended
AUTH_CHALLENGE_PASSCODE_STR does not exist - entry will be appended
AUTH_CHALLENGE_PASSWORD_STR does not exist - entry will be appended

************************************************************
* You have successfully installed RSA Authentication Agent 6.0 for PAM
************************************************************
```

SecurID Verification Test

Note that the test requires a user name and passcode <PIN + token code>.
As a root-privilege user, test PAM module as shown below:

```
# cd /opt/pam/bin/
# ./acetest
Enter USERNAME: <username>
Enter PASSCODE: <PIN + token code>
```

The result should be successful (as indicated below) if the user credential is correct.

```
Authentication successful.
```

Note that in some cases, the RSA SecurID token is in the status of "next tokencode" mode. If that is the case, the test session will look like this:

```
# ./acetest
Enter USERNAME: <user_id>
Enter PASSCODE: <PIN + tokencode1>
Wait for the tokencode to change,
then enter the new tokencode: <tokencode2>
Authentication successful.
```

If authentication testing is not successful, please contact The JPL Service Desk.

Configuration PAM to support SSH Server with SecurID Credentials

```
# cd /etc/pam.d
# vi sshd
```

(Comment the line and insert the 2nd line as given below.)

```
#auth       required     pam_stack.so service=system-auth
auth       required     pam_securid.so
```

(Save file and exit.)

Configuration SSH Server with SecurID Credentials

```
# cd /etc/ssh
# vi sshd_config
```

(Modify the lines as given below.)

```
#PermitRootLogin yes
PermitRootLogin no

# PasswordAuthentication yes
PasswordAuthentication no
```

```
#ChallengeResponseAuthentication no
ChallengeResponseAuthentication yes

UsePrivilegeSeparation no
```

(Save file and exit.)

```
# /etc/init.d/sshd restart
```

SSH Client Verification Test

DO NOT CLOSE THE WINDOW UNTIL YOU'VE CONFIRMED THAT AUTHENTICATION IS WORKING PROPERLY.
With the current root window still open, on a separate SSH client, login to the host on which the Authentication Agent is installed and PAM module is configured. The login should prompt for **PASSCODE** after username is entered.